T4 初めての人のためのインターネットルーティング

クラウド事業者における トラフィックトレンド

さくらインターネット研究所 大久保 修一
ohkubo@sakura.ad.jp
AS9370, AS9371, AS7684

自己紹介

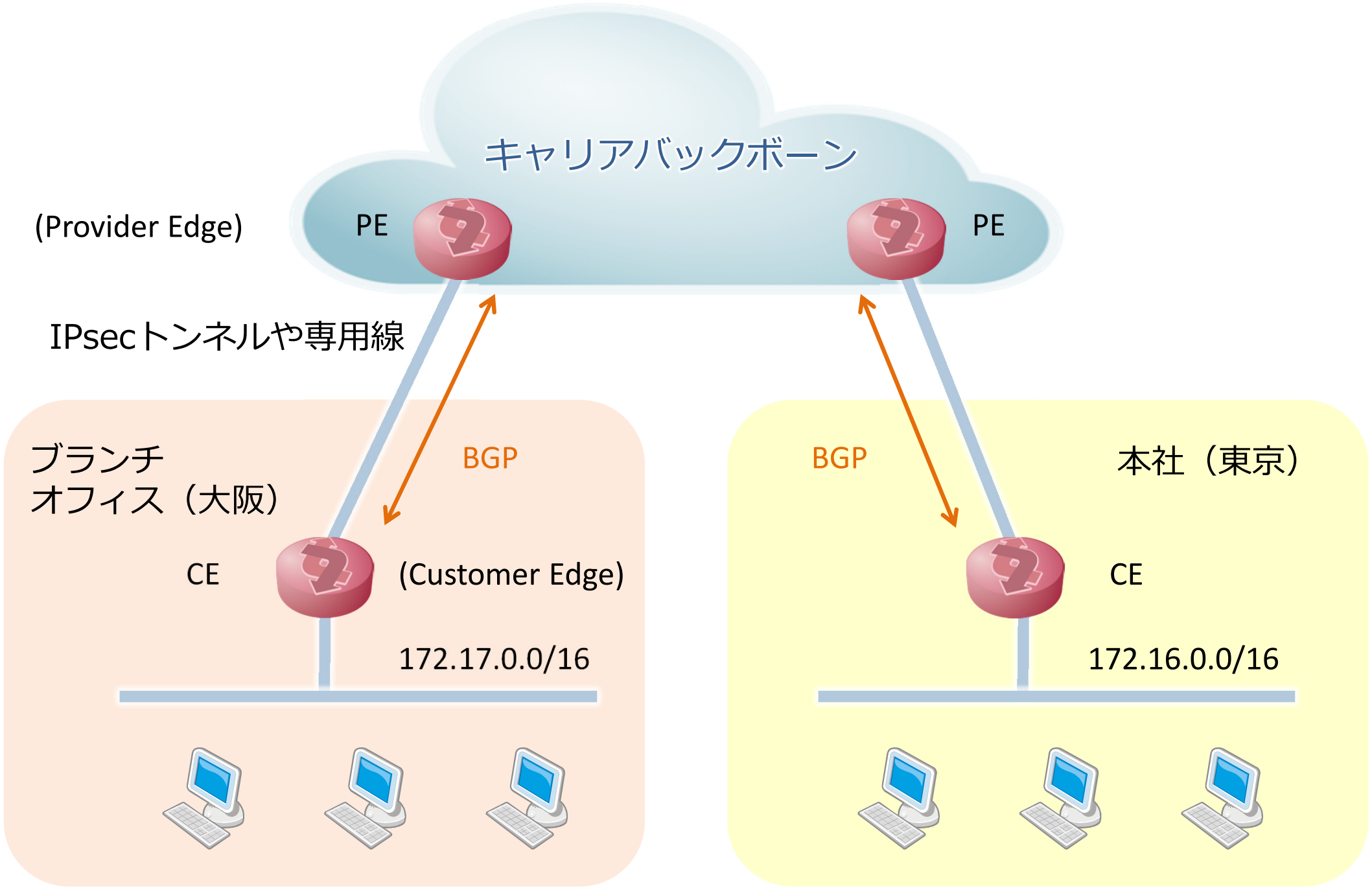
SAKURA Internet

- 2003/4 さくらインターネット入社
  - バックボーンネットワークの運用を担当
- 2009/7 さくらインターネット研究所
  - IPv4アドレス枯渇対策、クラウド技術等の研究活動
- 2011/3～ 「さくらのクラウド」の開発に参加
  - インフラ開発を主に担当
- 著書：オープンソース・ソフトウェアルータVyatta入門(共著 2011/6)

- Interop Tokyo 2013, 2014, 2015
  ShowNet NOCメンバー
- 好きなルーティングプロトコル：BGP

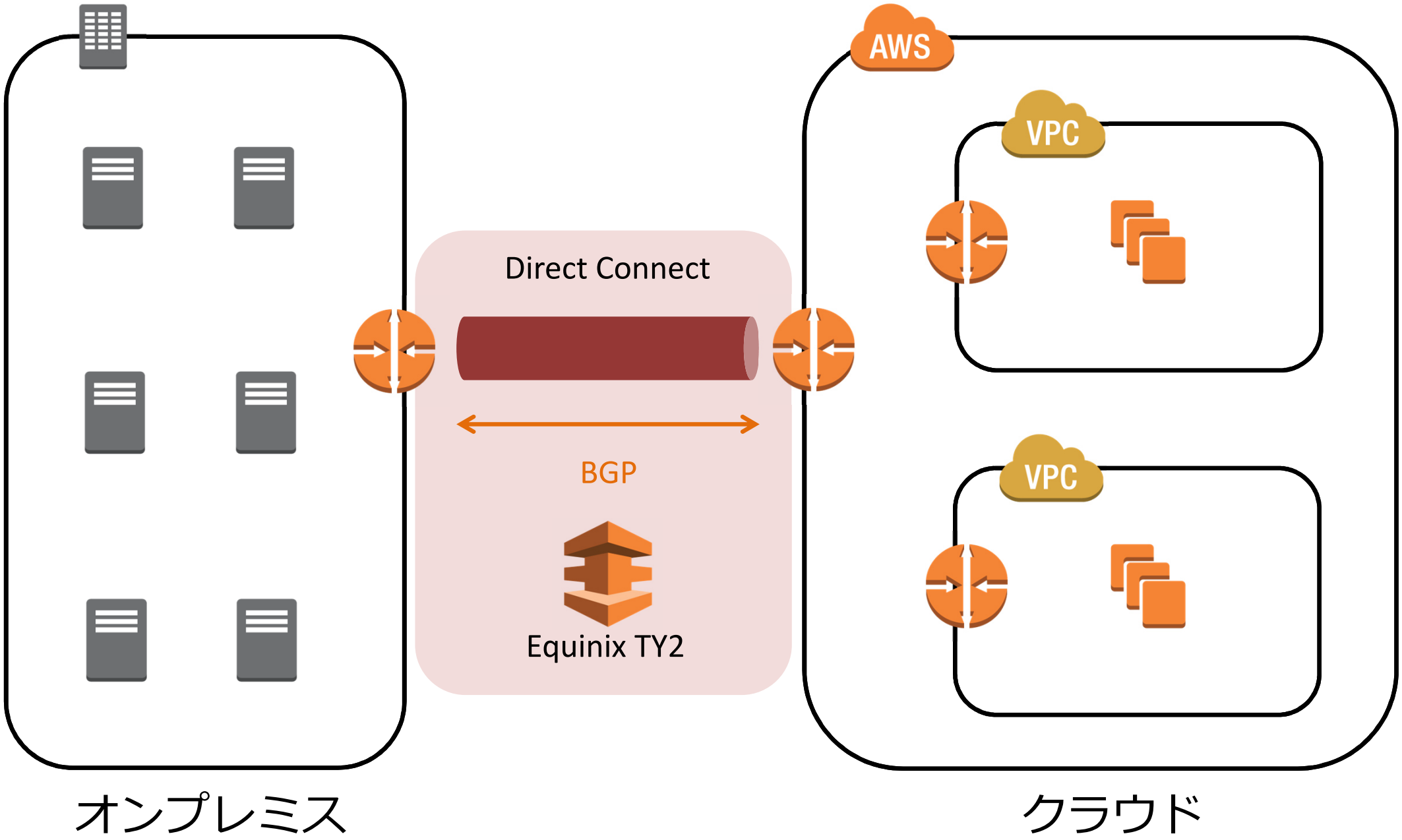
BGPはインターネットバックボーン以外でも
広く使われるようになってきています。

IP-VPNエッジでのBGP利用例



AWS Direct Connectの例

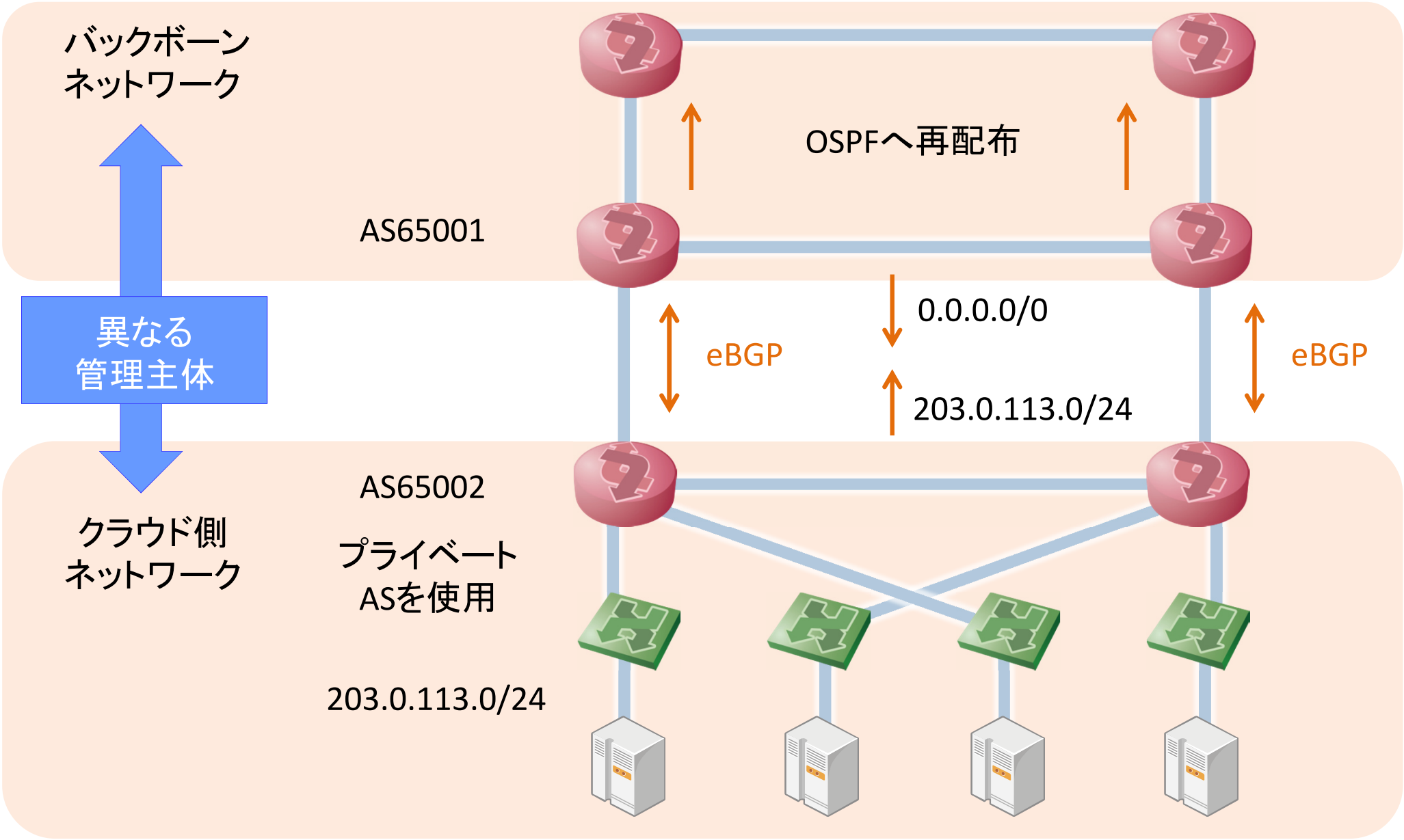
SAKURA Internet



組織内におけるBGPの活用

SAKURA Internet

弊社のIaaS「さくらのクラウド」でのバックボーンとのルーティング構成の例



BGPが便利なケース

SAKURA Internet

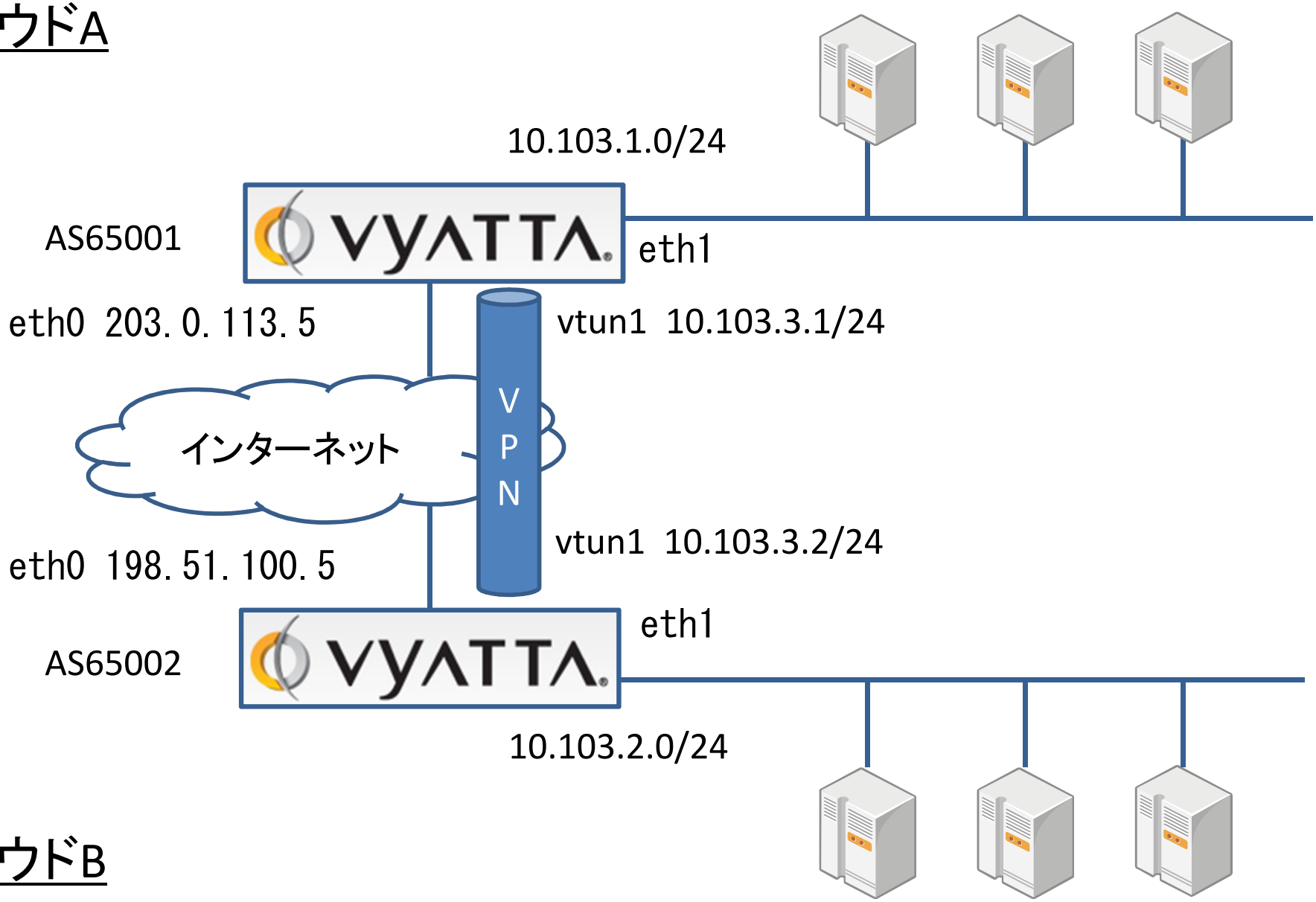
- 組織内でも異なる管理主体の場合
  - 元々グローバルAS間の接続もそうだった
- OSPFでは異常経路のフィルタができない
  - エッジまで管理できることが前提
- 「さくらのクラウド」での事情
  1. お客様がコンパネから仮想ネットワークの申し込み
  2. コントローラがルータに自動的に設定投入
  3. プログラムバグ等で不正な経路がバックボーンに広報されるとルーティング障害になってしまう
  4. BGPのIngress経路フィルタで防ぐ

身近な部分でも利用されているので
是非覚えておきましょう

かんたんなBGPの設定例

SAKURA Internet

クラウドA



クラウドB

片方のVyattaにて

```
$ generate openvpn key /config/auth/secret
$ sudo scp /config/auth/secret vyatta@198.51.100.5:/config/auth/
```

双方のVyattaにて（クラウドA側の例）

```
edit interfaces openvpn vtun1
set local-address 10.103.3.1 subnet-mask 255.255.255.0
set mode site-to-site
set remote-address 10.103.3.2
set remote-host 198.51.100.5
set shared-secret-key-file /config/auth/secret
top

edit protocols bgp 65001
set neighbor 10.103.3.2 remote-as 65002
set neighbor 10.103.3.2 soft-reconfiguration inbound
set network 10.103.1.0/24
commit
```

※ クラウドB側は**赤字**の部分を変更する

弊社における
トラフィックトレンド

・・・の前に

弊社のデータセンターサービスを
簡単に紹介させてください。

さくらインターネットのサービス

SAKURA Internet

ハウジングサービス

ハウジング

リモートハウジング

データセンターへの入局や機器の設置といった物理作業のすべてを代行するサービス

※石狩データセンターで提供

専用サーバサービス

さくらの専用サーバ sakura dedicated server

専用サーバ Platform St

専用サーバ Platform Ad

1台 ～ 複数台

クラウドサービス

さくらのクラウド sakura cloud

高性能サーバと拡張性の高いネットワークを圧倒的なコストパフォーマンスで実現

仮想サーバサービス

さくらのVPS

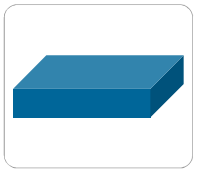
仮想化技術を用いて、1台の物理サーバ上に複数の仮想サーバを構築し、仮想専用サーバとして利用するサービス

レンタルサーバサービス

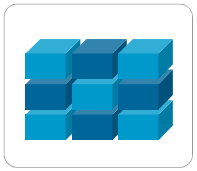
さくらのマネージドサーバ

さくらのレンタルサーバ

1台を専有



1台を共有



・サービスの主な利用用途

エンタープライズ

SNS、Webアプリケーション、SaaS、ASP

会員制サイト、キャンペーンサイト

ネットビジネス、電子商取引、動画・音楽配信

インターネットメール、Webサイト運営

データセンターの概要

SAKURA Internet

業界トレンドと幅広い利用者からのニーズを反映したデータセンター

様々なサービスが集約できる
国内最大級の拡張性を持つ**郊外型データセンター**

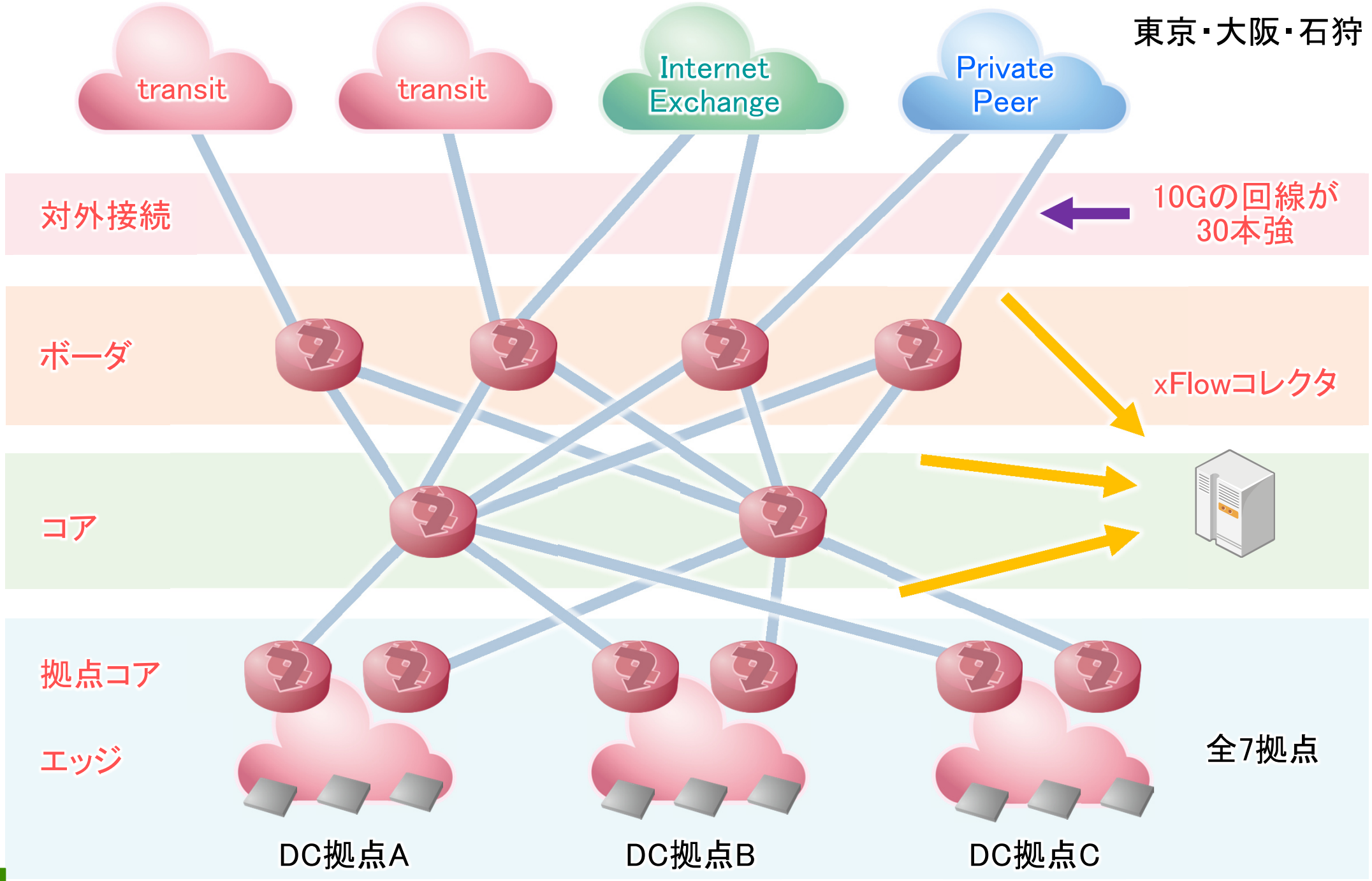
オフィス至近、豊富な配信実績を持つ
都市型データセンター

●用途
ハウジング、ホスティング、クラウド

●総ラック数
2,700基(2014年3月現在)

●顧客数
325,000件(2014年3月現在)

バックボーン構成イメージ



トラフィック計測方法

SAKURA Internet

- 全てのボーダルータ、コアルータにて
- 主にsFlowを用いた計測
- フローサンプルをコレクタに飛ばし、各種統計データを算出
- 取得しているデータ
  - AS別のトラフィック流量
  - Prefix別のトラフィック流量(一部ASが対象)
  - DoSアタック、異常トラフィックの検出
  - その他
- いずれも、障害の低減、安定したサービス提供、円滑なバックボーン運用を助ける目的

トラフィック
トレンドその１

配信トラフィックの
宛先AS別流量

宛先AS別トラフィック(2014/10)

SAKURA Internet

会場のみ

宛先AS別トラフィック(2006/9)

SAKURA Internet

会場のみ

ここ数年の傾向

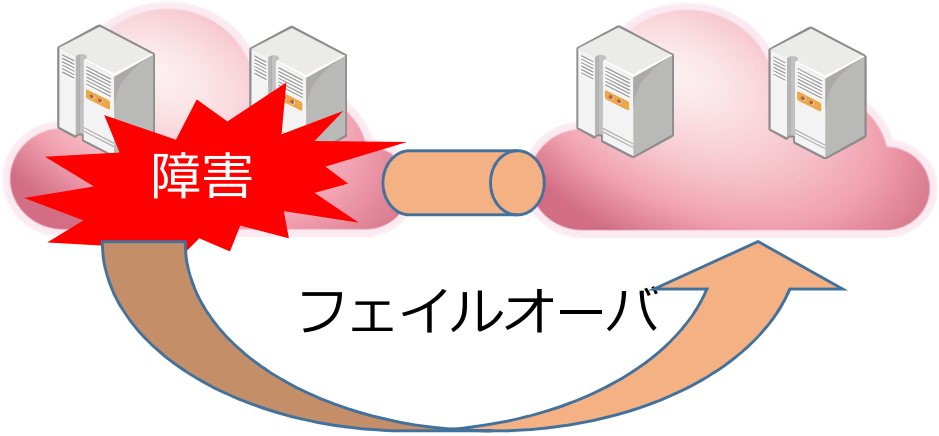
SAKURA Internet

- 固定サービスのISPさん向けの配信トラフィックは、絶対量としては相変わらず最多
- ここ数年、モバイル3社向けが顕著な伸び
  - スマートフォンの普及による
- 12:00-13:00の間の伸び(ほぼモバイルの影響)
- CDN事業者向けも若干目立つ
  - Originサイトとしての利用？
- サーバ間(クラウド間)のトラフィックもちょいちょい増えている
  - マルチクラウドの潮流

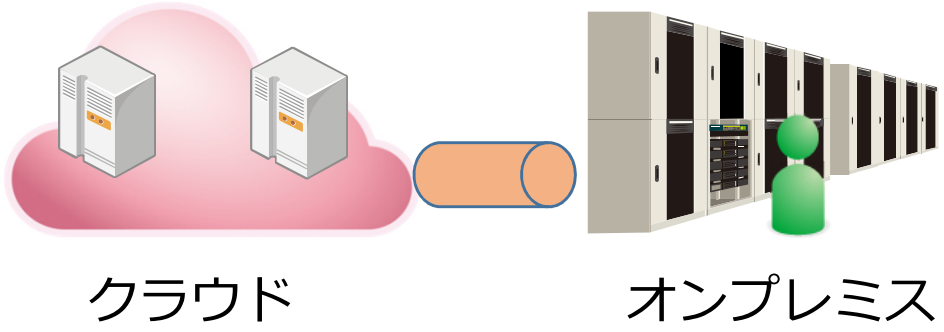
マルチクラウド利用の広まり

SAKURA Internet

障害、災害対策



オンプレミスとの併用



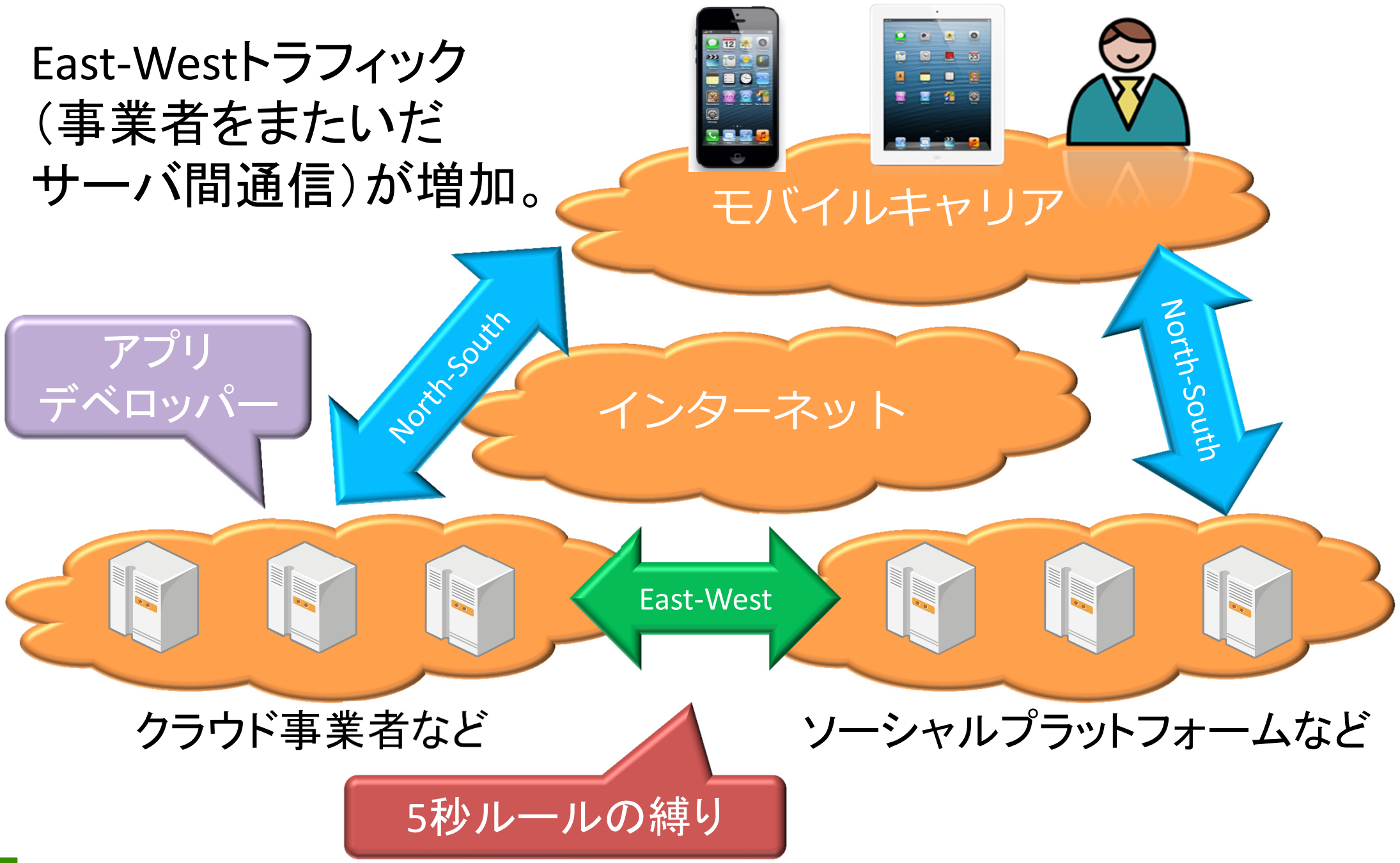
マルチクラウド活用のメリット

- 障害、災害対策
- ワークロード分散
- オンプレミスとの併用
- コスト削減
- ベンダーロックインの回避
- クラウドのいいとこ取り

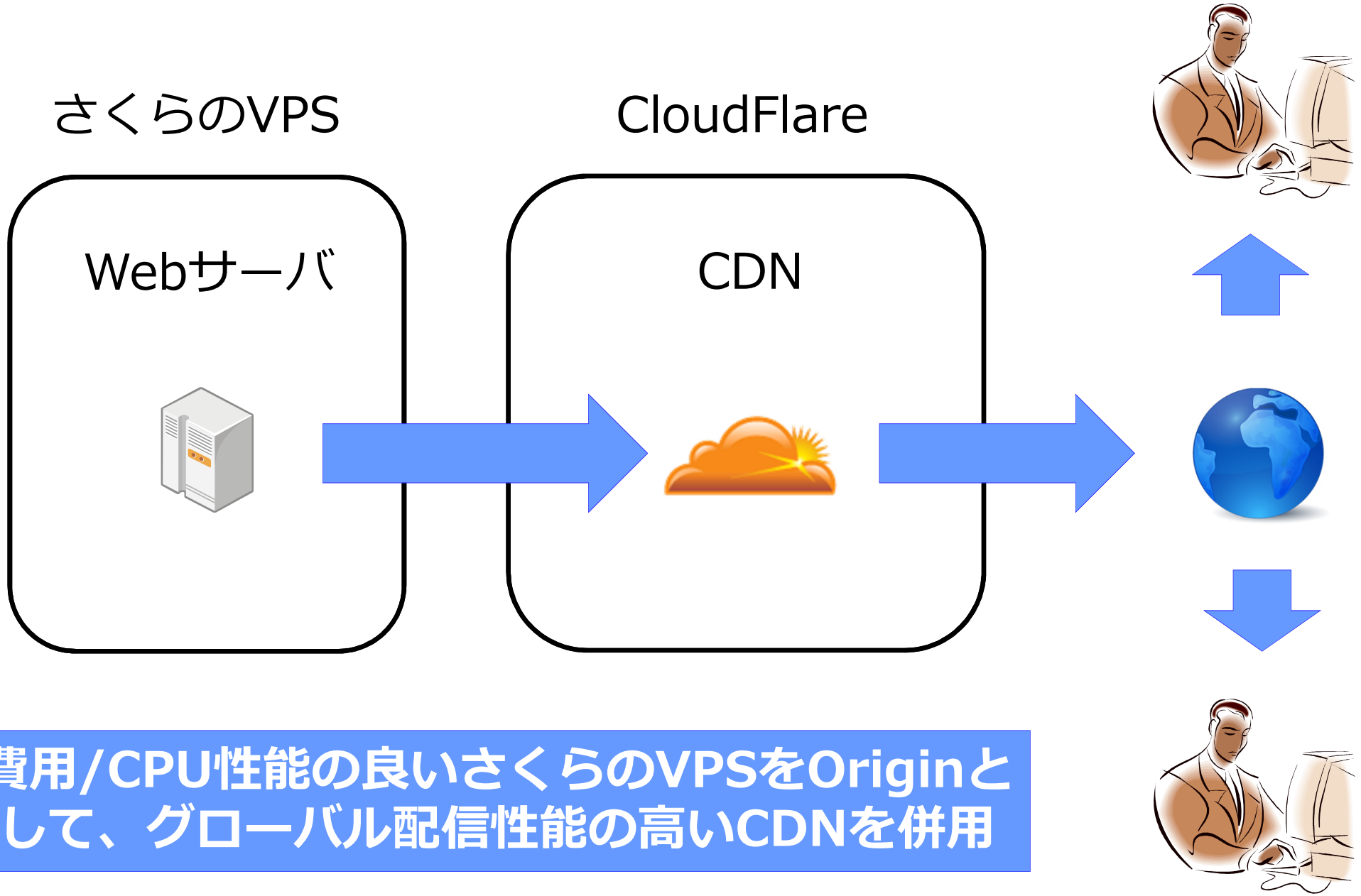
East-Westトラフィックの増加

SAKURA Internet

East-Westトラフィック
（事業者をまたいだ
サーバ間通信）が増加。

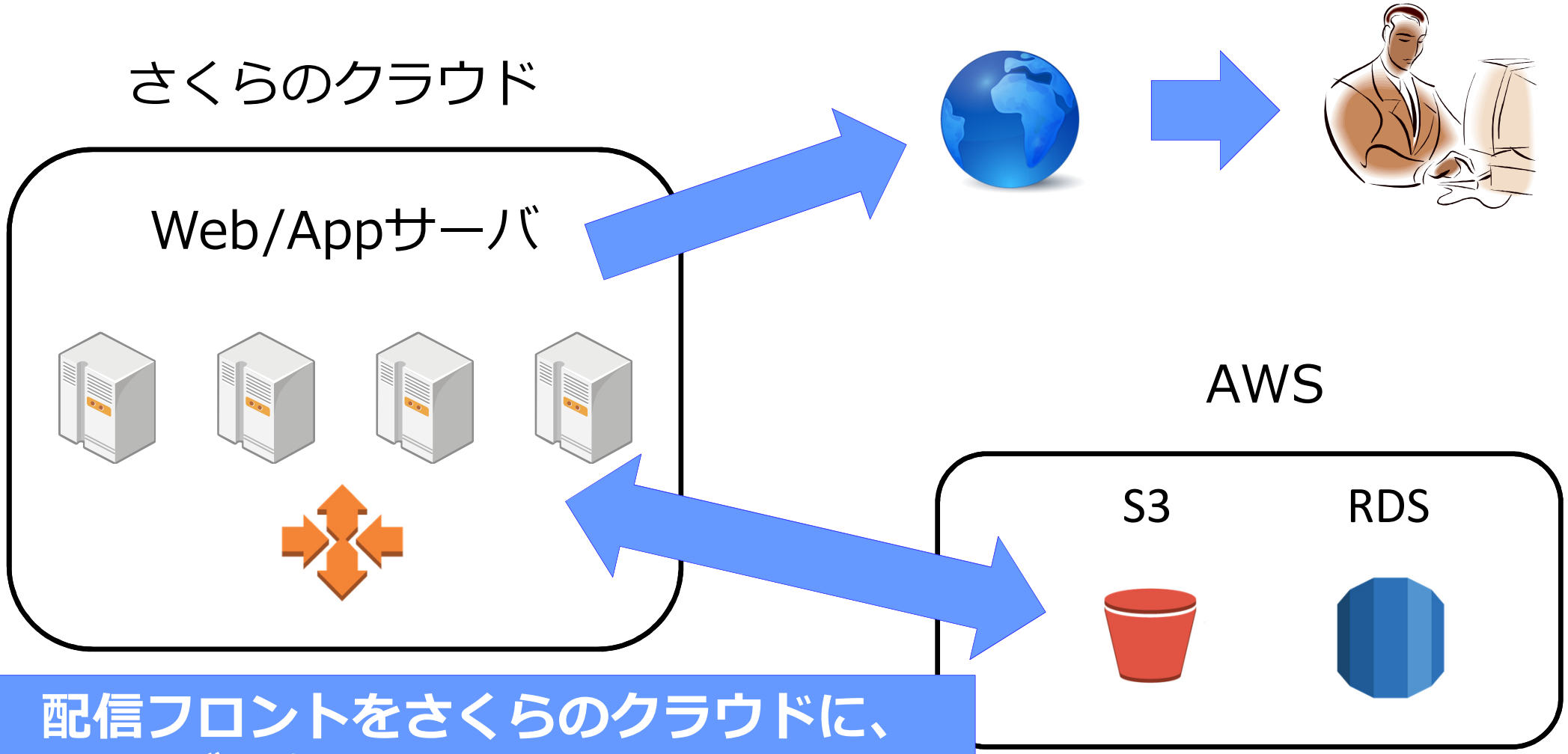


さくらのVPSとCloudFlareを併用



費用/CPU性能の良いさくらのVPSをOriginとして、グローバル配信性能の高いCDNを併用

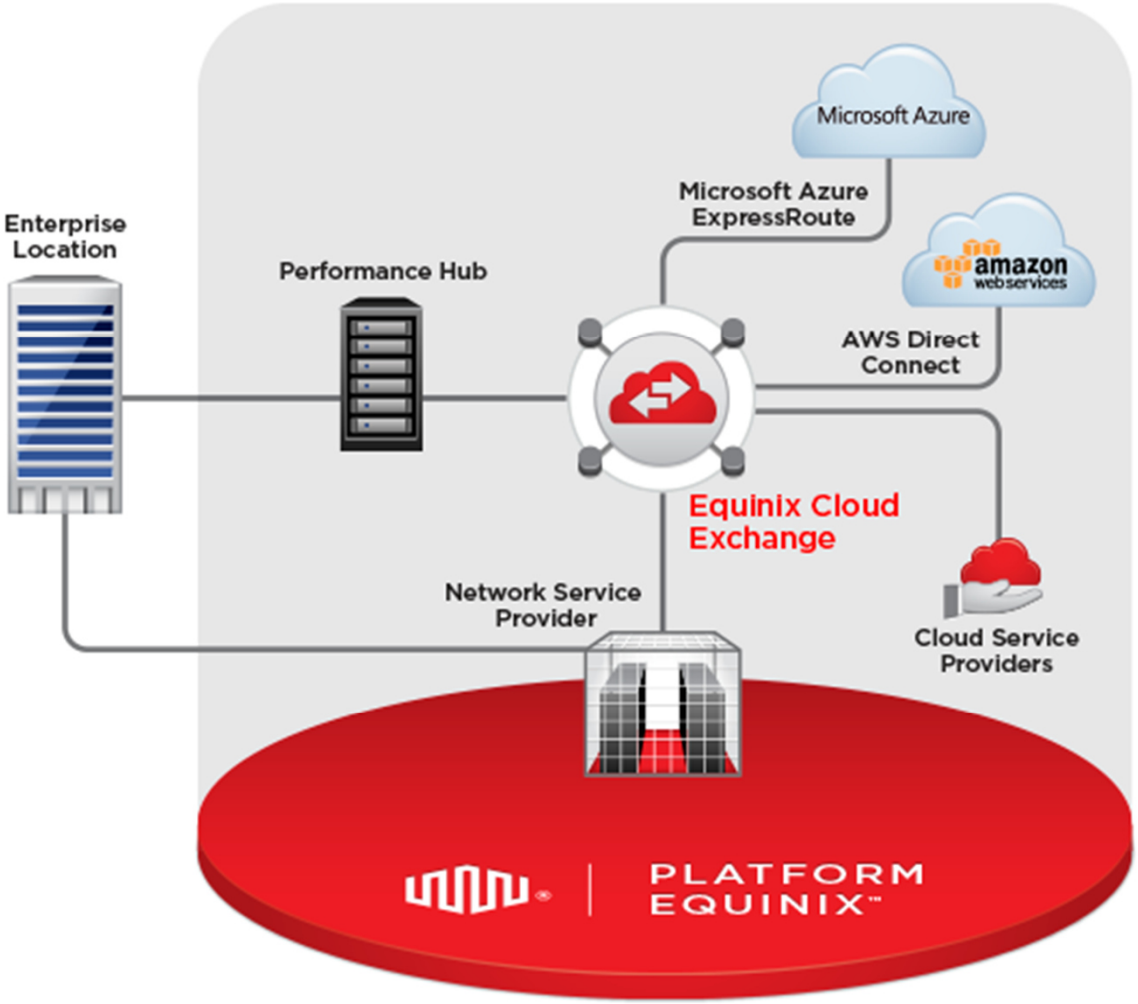
さくらのクラウドとAWSを併用



**配信フロントをさくらのクラウドに、
ログ保存、DB管理をAWSに。
流量一定の場合はトラフィックコストを
圧縮可能**

Equinix Cloud Exchangeの例

SAKURA Internet



Equinix Cloud Exchangeの特長

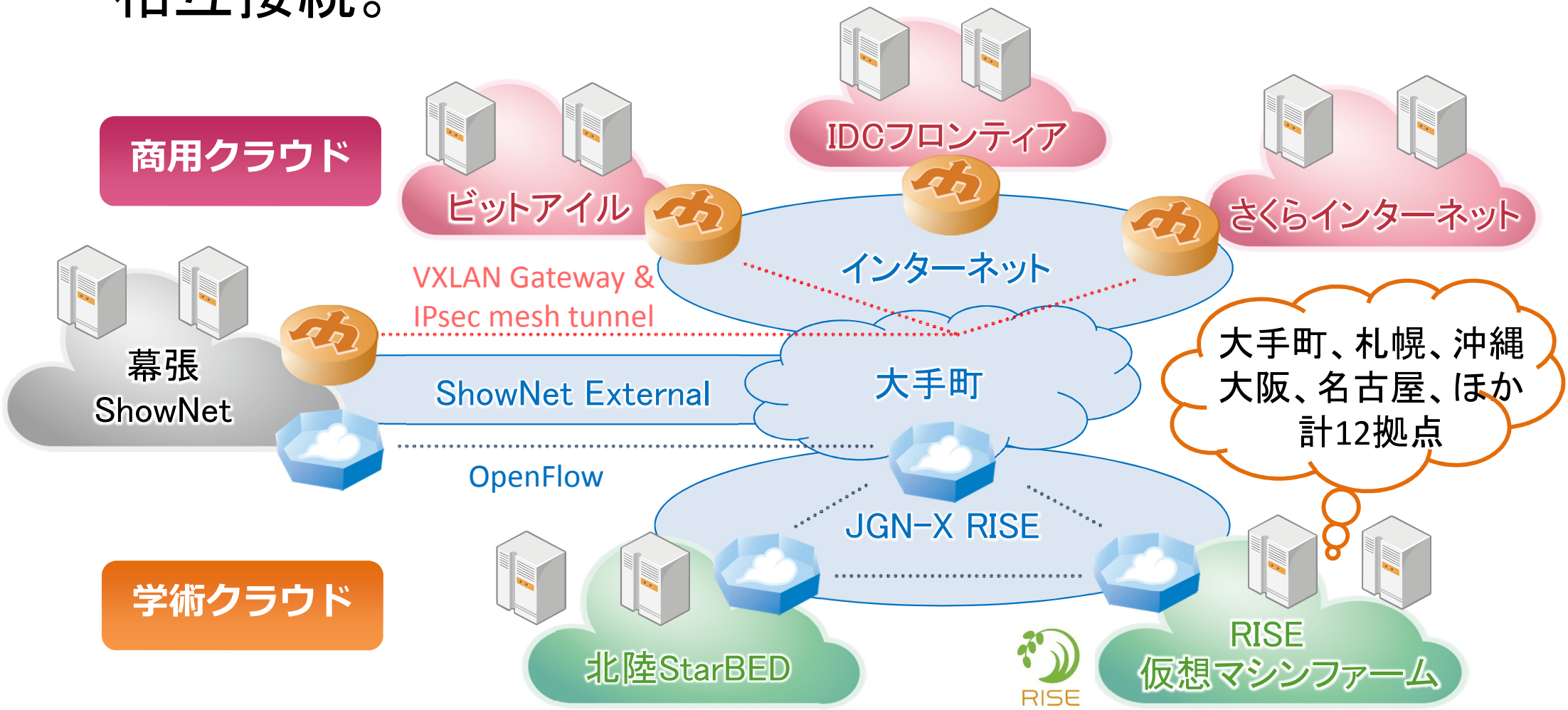
- セキュアで、ハイパフォーマンスの接続– Equinix Cloud Exchangeは、インターネットを介さず、仮想プライベート直接接続により、幅広い帯域の選択肢と共により高いセキュリティとパフォーマンスを提供します。
- オンデマンドで自動化されたクラウド接続 – Equinix Cloud Exchangeポータルおよびapiによって、複数のクラウドサービスおよびネットワークへの接続プロビジョニングと管理プロセスを簡単に行うことができます。
- 1ポートで複数のバーチャルサーキット– 単一の物理ポートを通して多くの参加者（クラウド、ネットワーク、企業のお客様）へ接続し、さまざまな当事者間でダイナミックに帯域を割り当てることができます。
- 世界中でご利用可能– Equinix Cloud Exchangeは、世界のトップ17のビジネス市場でご利用になれます。
- 最大のクラウドエコシステム– Equinix Cloud Exchangeは、AWSおよびMicrosoft Azureを含む、データセンターサービス業界でもっとも広範なクラウドサービスとの接続を提供しています。

http://www.equinix.co.jp/services/interconnection-connectivity/cloud-exchange/ より

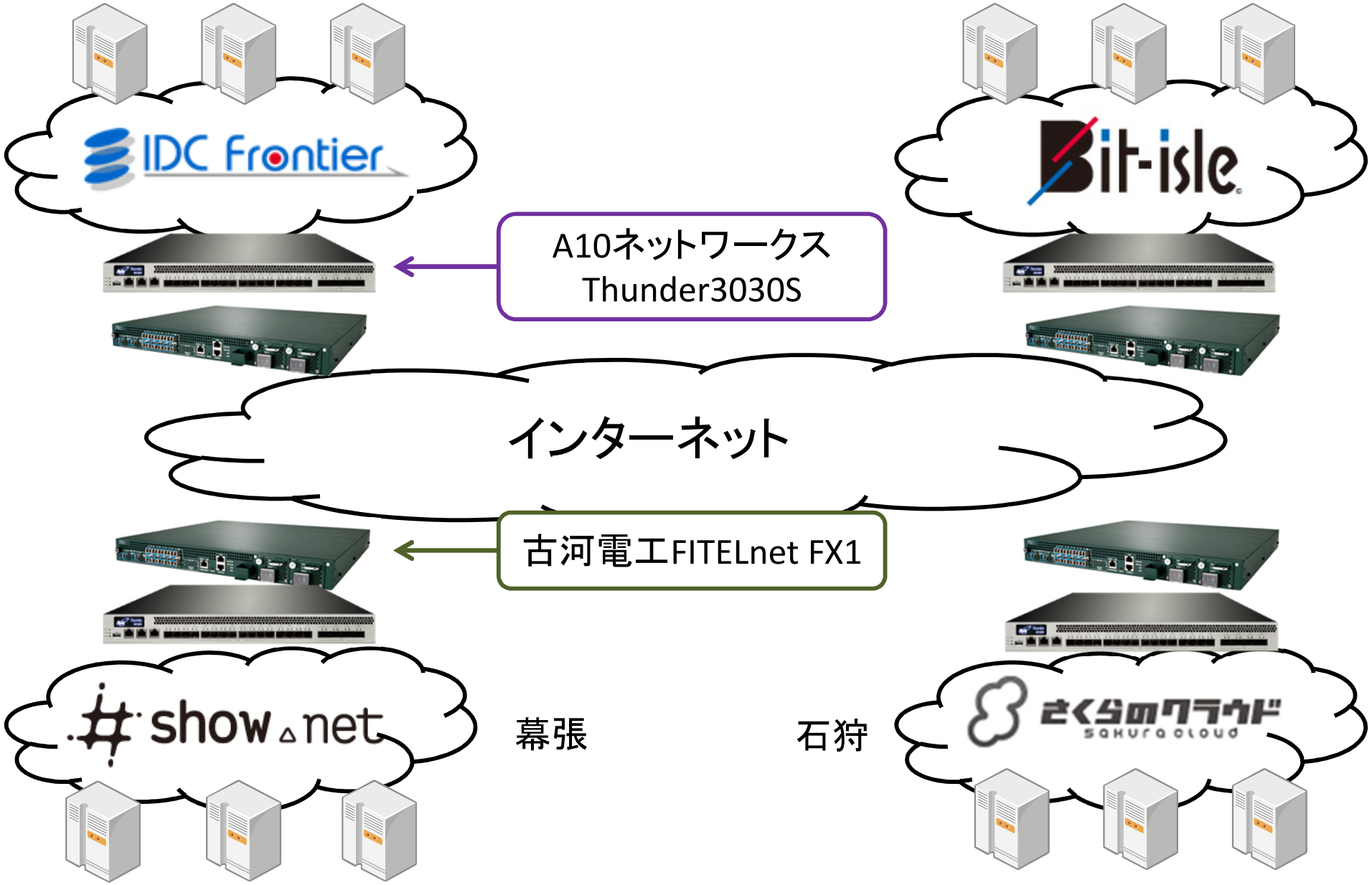
国内事例：Interopでのインタークラウド実験

SAKURA Internet

商用クラウド3社と、StarBEDをはじめ国内12拠点にまたがるRISE仮想マシンファームを、ShowNetにて相互接続。



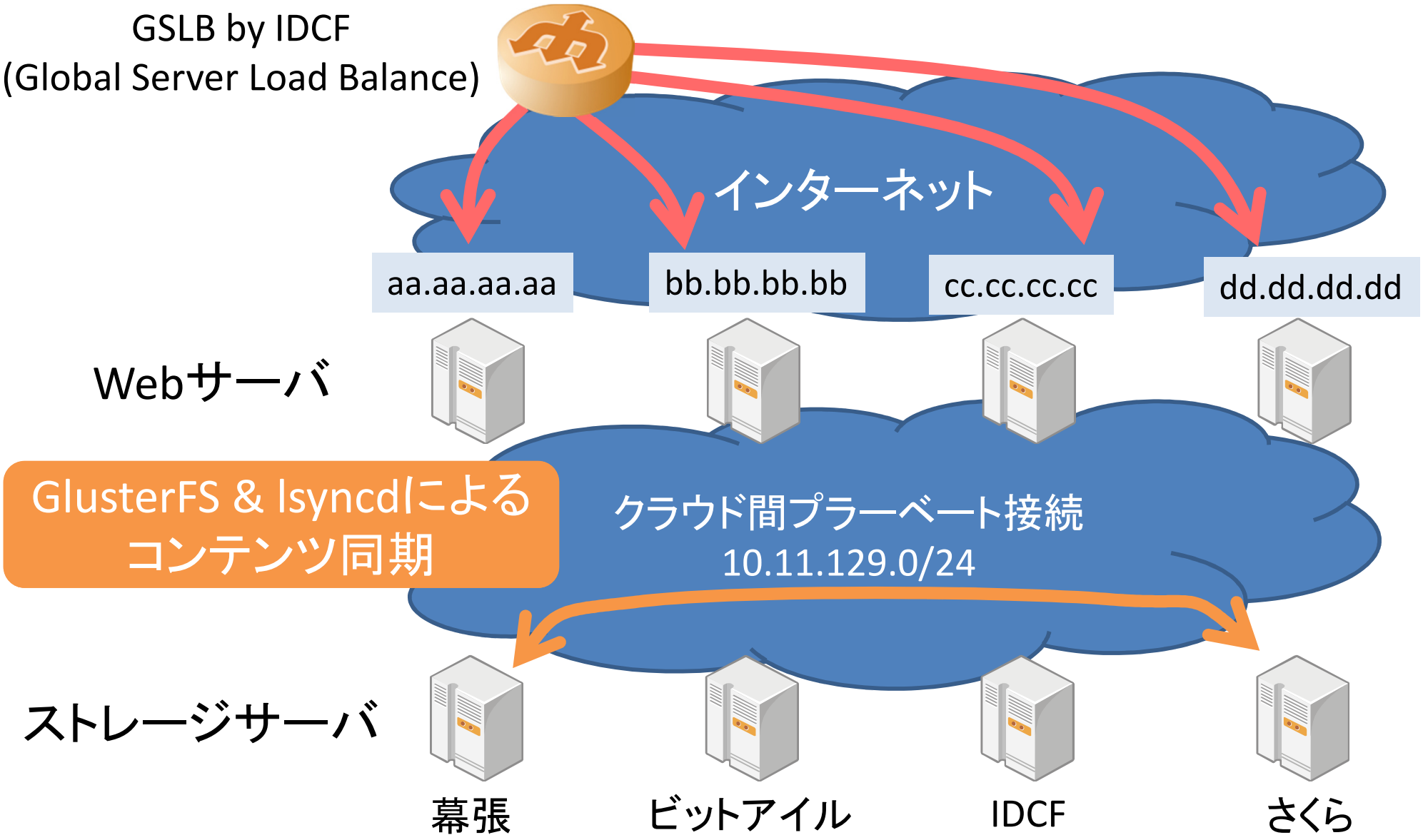
商用クラウド側の接続構成



SAKURA Internet

デモンストレーション内容

GSLB by IDCF
(Global Server Load Balance)



事業者間トラフィックの将来予想

SAKURA Internet

- モバイル向けは今後も増加？
- クラウド間接続を例とした、インターネットを経由しないトラフィック流通の要望が増すのでは？
- 従来ローカルでやりとりされていたサーバ間通信を事業者を超えて実現する高い品質が要求される
- セキュアでロバストなセミクローズド接続の実現に向けた取り組みが必要
  - クラウド事業者も回線キャリアの視点が必要？

トラフィック
トレンドその２

配信トラフィックの
ソースポート番号別流量

ソースポート番号別トラフィック(2014/10)

SAKURA Internet

会場のみ

ソースポート番号別トラフィック(2006/9)

SAKURA Internet

会場のみ

ソースポート番号から見た最近の傾向

SAKURA Internet

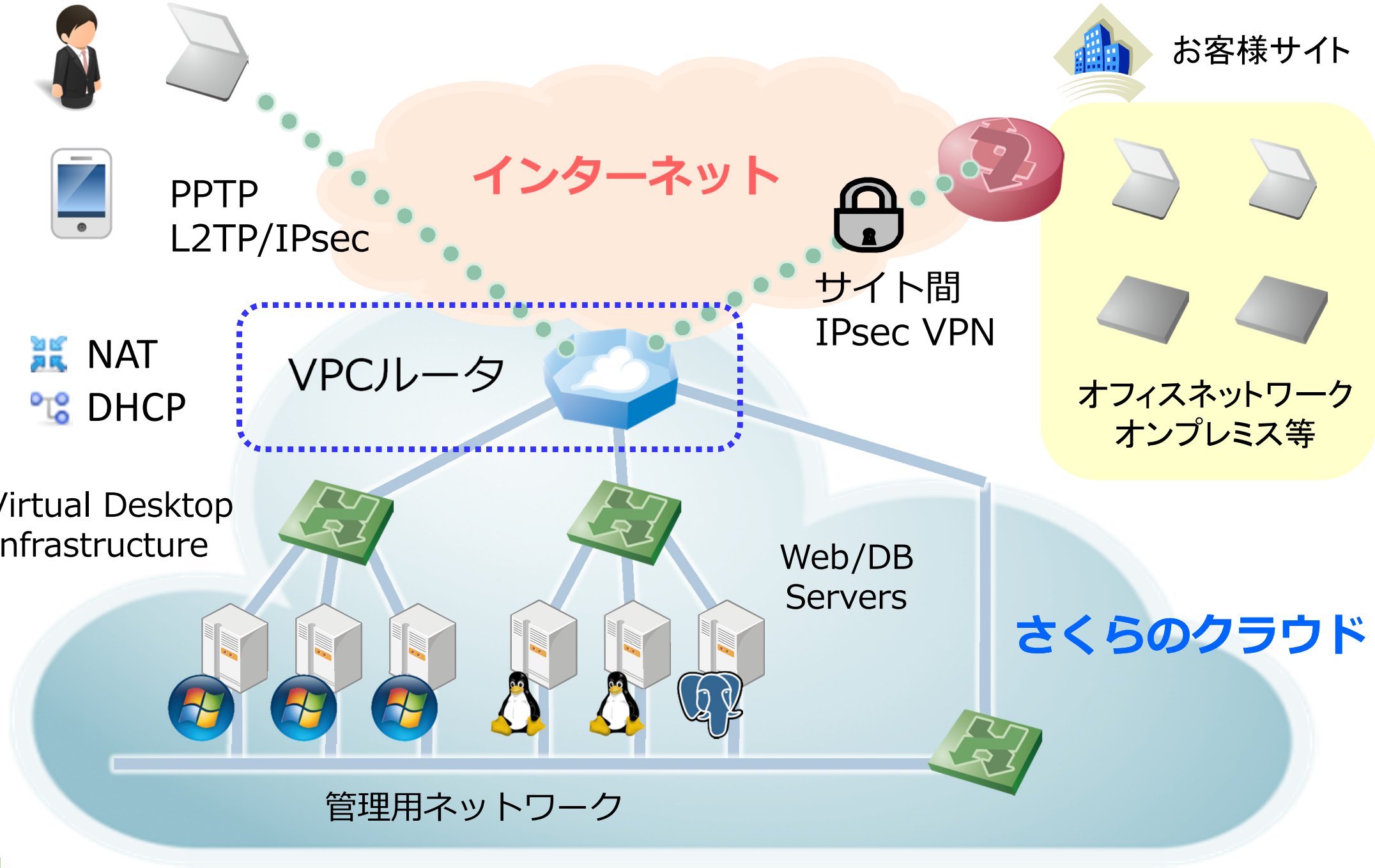
- 相変わらず80番ポートからのトラフィックが圧倒的に多い
  - 最近では、様々なアプリケーションがHTTPに乗ってきているため、Web以外の用途も多いと思われる。
  - 動画ストリーミングも80番ポートに移っている？
- 絶対量は少ないが、443番ポート(HTTPS)の比率は以前より増加。
- 今後、Webの暗号化通信が一層増加？
  - SPDYやHTTP2.0の普及によっても増える可能性
- 案外DBポートが目立つ
  - サーバ間の通信の一例

ソースポート番号から見た最近の傾向

SAKURA Internet

- 現時点でも123番ポート(NTP)がちょいちょい存在(一時は膨大な量となった)
- VPN系のポート番号も若干
  - バーチャルプライベートクラウド環境へのアクセス
- 加えて、今後IoT(Internet of Things)の広まりにより、デバイスが生成するデータの受け皿としてクラウド基盤の活用が進むか？
- IoTによって膨大なトラフィックを生む可能性

IaaS上でのプライベートクラウド環境構築例



IoTとは？

SAKURA Internet

- IoT = Internet of Things
- 直訳すると”モノ”のインターネット
- 携帯端末、家電、センサーなどのデバイスがインターネットに接続されてくる。
- 人間の操作によって生成されていた従来ながらのトラフィックだけでなく、そういったデバイスが生成するトラフィックがインターネット上を往来する。
- 技術的な規格には・・
  - IEEE802.15.4
  - 6LoWPAN(RFC6282)、その他
- 低コスト、低消費電力、近距離無線通信

IoT的なクラウドのユースケース

SAKURA Internet

会場のみ

IoT的なクラウドのユースケース

SAKURA Internet

会場のみ

IoT的なクラウドのユースケース

SAKURA Internet

会場のみ

ルーティングの観点からみた不正トラフィック/DoSアタック対策

不正トラフィックの例

SAKURA Internet

- インターネットから受けるDoSアタック
- インターネット向けに発信されるDoSアタック
- DNS/NTP等のampアタック

トラフィックボリューム：比較的大
第三者通信への影響：比較的大
バックボーンネットワークでの対応が必要

- SPAMメール、ウィルスメール送受信
- SSHブルートフォースアタック等のscan攻撃
- OSやミドルウェア等特定脆弱性をついた攻撃

トラフィックボリューム：比較的少
第三者通信への影響：比較的少
エッジでのFW, IPS, セキュリティソフト等での防御

NTP AMPアタックのトラフィック傾向

SAKURA Internet

会場のみ

サーバセキュリティの問題

SAKURA Internet

会場のみ

- クラウドやVPS等、気軽にサーバを作成できるようになった反面、推測されやすいパスワードを設定するなどで、セキュリティ的に脆弱な状態になりがち。

弊社におけるDoS攻撃に対する取組み

SAKURA Internet

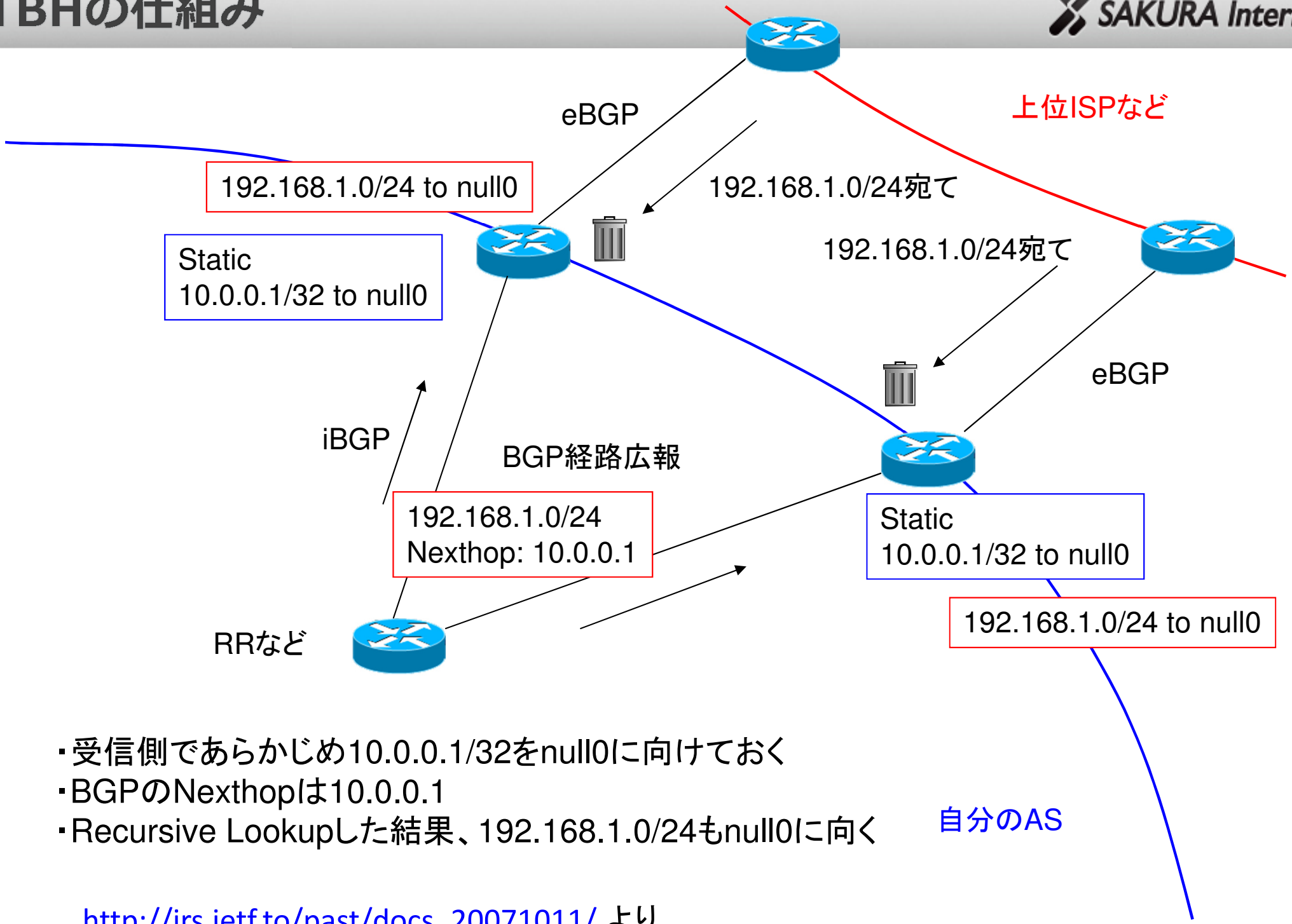
- 2007年頃にRTBHのシステムを構築
- RTBH ＝

  Remotely Triggered Black Hole Filteringの略
- BGPにてNexthopをnullに向けた経路を広報することにより、AS内の全BGPルータに、一斉にnull routingを設定できる。
- DoSアタックの対応方法の１つ

詳細はこちらをご覧ください
http://irs.ietf.to/past/docs_20071011/

RTBHの仕組み

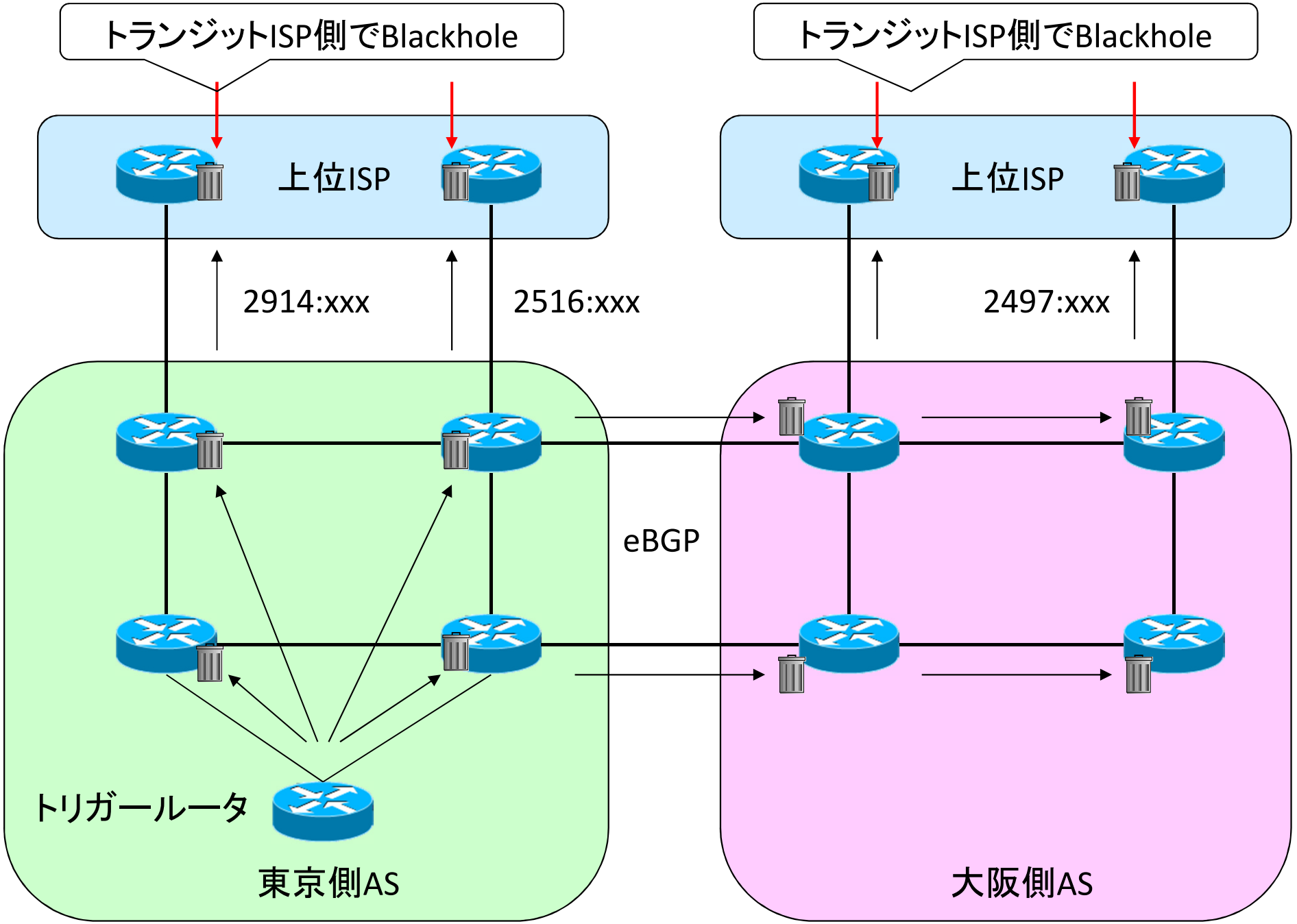
SAKURA Internet



・受信側であらかじめ10.0.0.1/32をnull0に向けておく
・BGPのNexthopは10.0.0.1
・Recursive Lookupした結果、192.168.1.0/24もnull0に向く

http://irs.ietf.to/past/docs_20071011/ より

トランジットISP向けのBlackhole経路伝達



RTBHの導入の効果

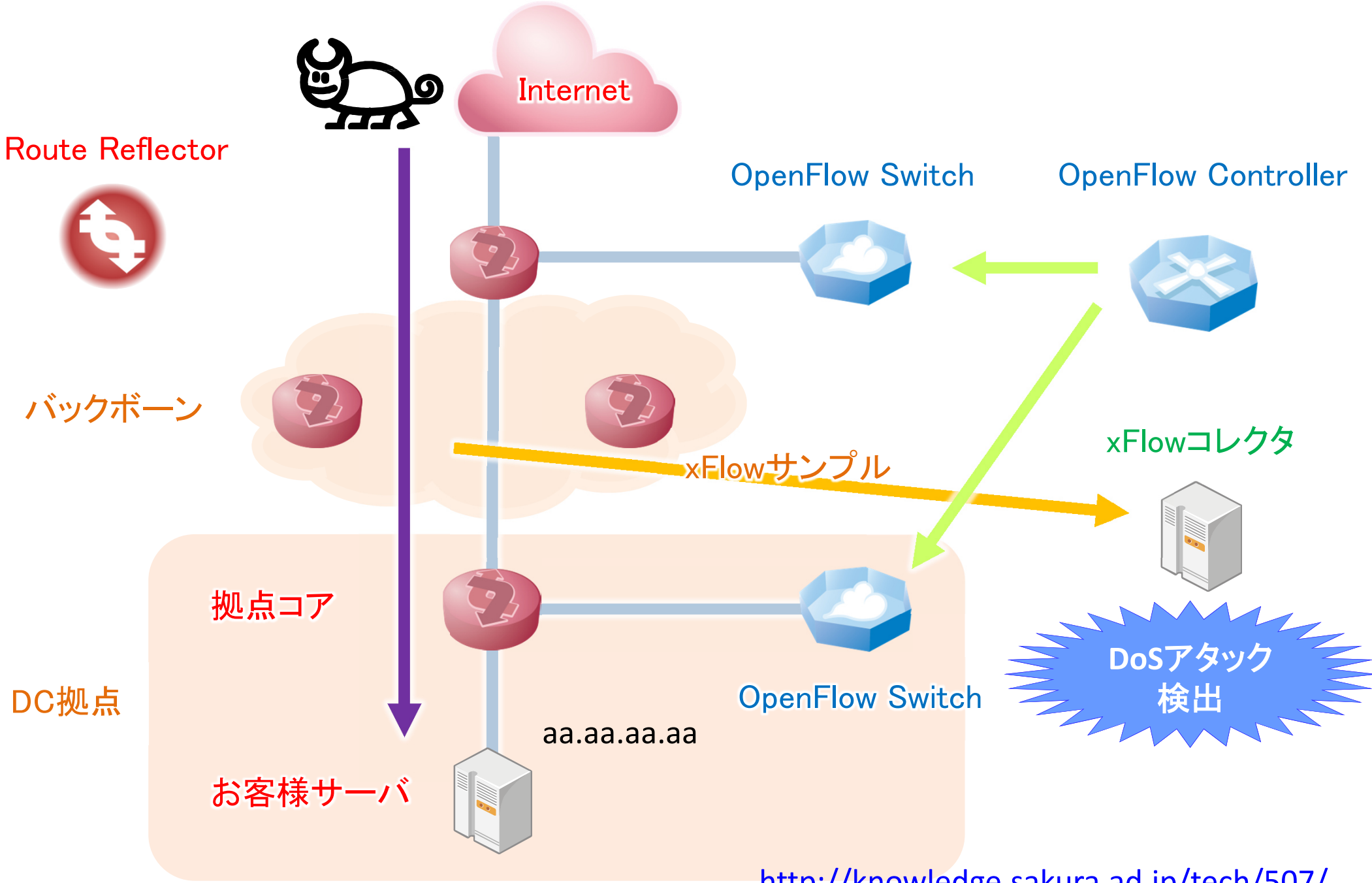
SAKURA Internet

- 大規模DoSアタックへの対応
  - 各ボーダルータでパケットフィルタすることにより、中継回線の輻輳を回避
- オペレーションの簡易化
  - 各ルータにACLを設定する場合に比べ、ミスをしにくく、設定をスピードアップ
- しかし、被害者向け通信はストップしてしまうため、DoS自体は成立してしまう問題

正常通信は通過し、不正トラフィックのみフィルタする仕組みが望まれる

DoSクリーニングシステム～2014年より運用開始

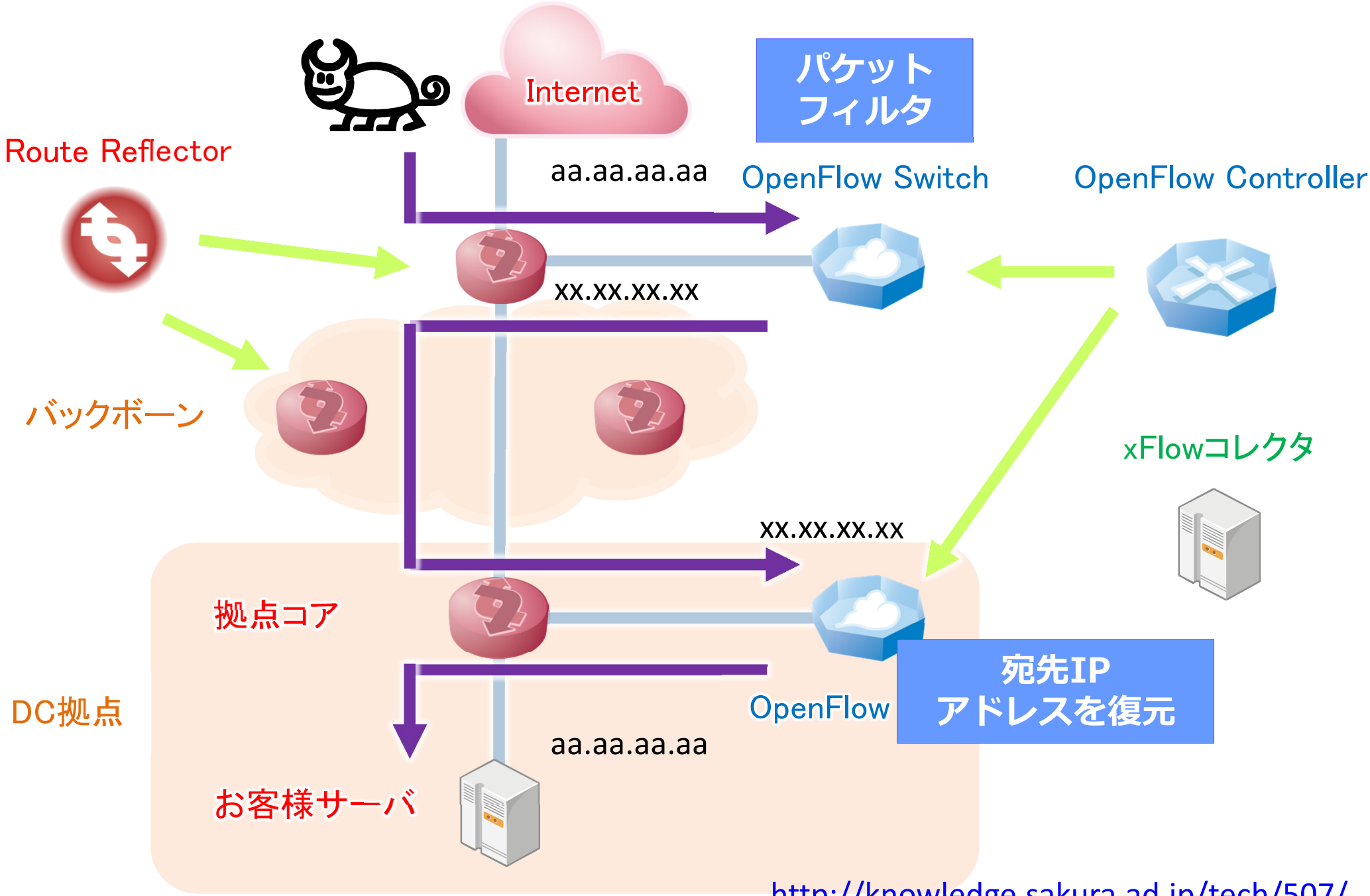
SAKURA Internet



http://knowledge.sakura.ad.jp/tech/507/

DoSクリーニングシステム～2014年より運用開始

SAKURA Internet



http://knowledge.sakura.ad.jp/tech/507/

導入の効果

SAKURA Internet

- 正常通信のみ許可し、不正トラフィックのみをフィルタ可能に(※)
- 特にレンタルサーバなどの共有ホスティング
  - 1つのIPアドレス(サーバ)に複数ユーザを収容
  - RTBHでそのIPアドレス宛の通信を止めると複数ユーザに巻き添えが及ぶ。
  - 巻き添えを防ぐために、以前はルータにACLを書いていたが、フィルタルールの一元管理が可能に。
- バックボーンに加え、各DC拠点にOpenFlow Switchが必要となる
  - その他BGP Flowspecを用いた実装手段も考えられる

※ 正常通信か不正通信かはネットワークサイドでは本当はわかりません。
※ 検出システムのシグネチャやオペレータによる複合的判断によるものです。

BGP Flowspec(RFC5575)

SAKURA Internet

- ざっくり言うと・・

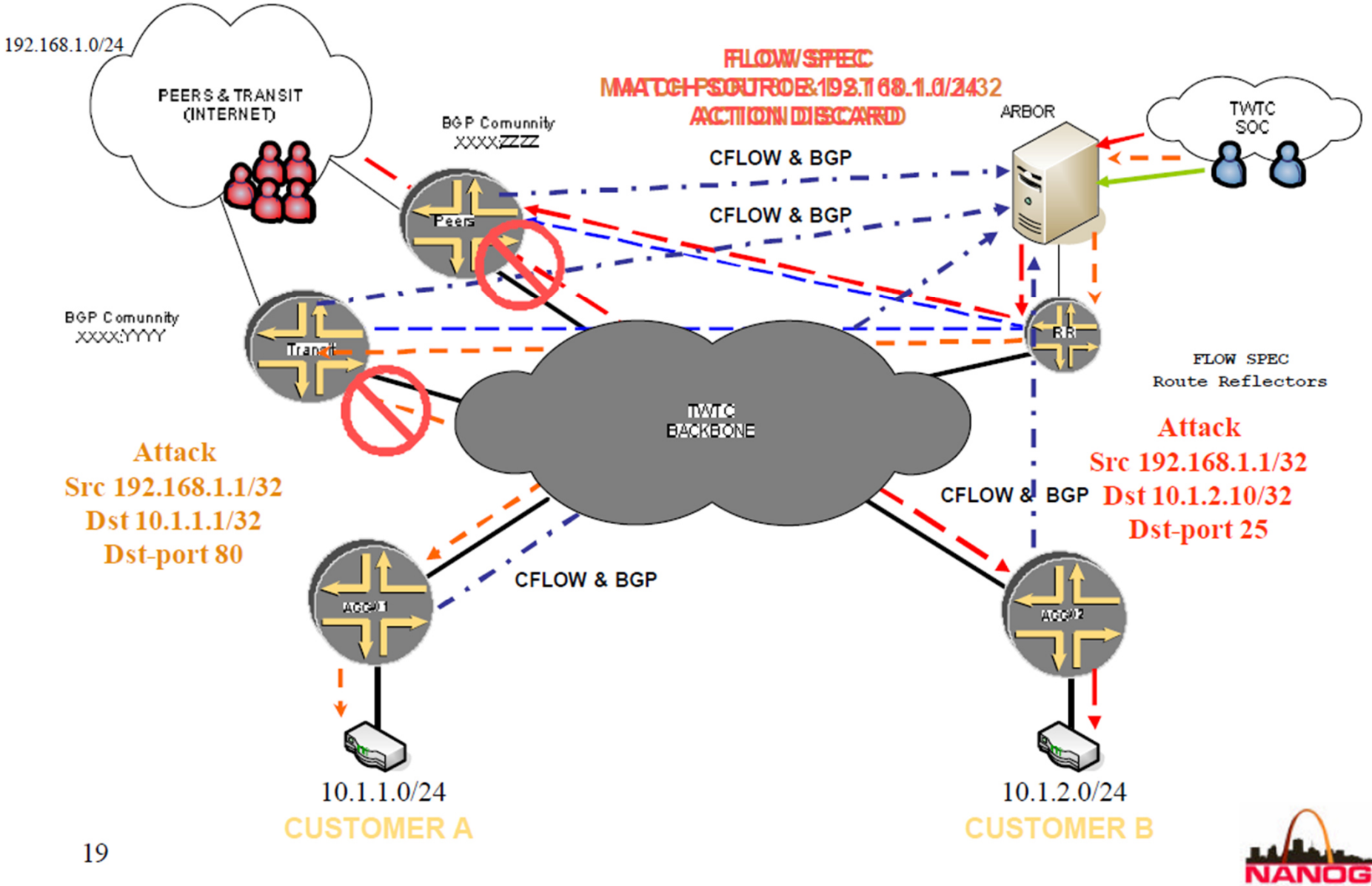
  ACL設定をBGPで網内のルータ群に配布するようなイメージ

- 従来のBlackhole/Sinkhole Routingでは、パケット中のIPアドレスに基づいたルーティング制御しかできない
- BGP Flowspecでは、パケット中の各フィールドの情報に基づいたフィルタリング等が可能
- 実装メーカ
  - Cisco, Juniper, Alcatel-Lucent

BGP Flowspecのデプロイ例

SAKURA Internet

Time Warner Telecom社の事例 (NANOG38 2006/10資料より引用)



http://www.monkey.org/~labovit/papers/labovitz-bgp-flowspec.pdf より

BGP Flowspec(RFC5575)

SAKURA Internet

- ルール指定可能なフィールド(IPv4/IPv6)
  - 送信元/宛先Prefix
  - IP Protocol (UDP, TCP, ICMP, etc…)
  - 送信元/宛先Port番号
  - ICMP Type/Code
  - TCP Flags
  - Packet Length
  - DSCP
  - IP Fragment
- 設定可能なアクション
  - 通過/レートリミット/破棄
  - VRFへのリダイレクト
  - DSCPマーキング
  - サンプリング/ロギング

※ いずれもプロトコル上の規定に存在するものであり、実装状況はメーカ/機種により異なります。

まとめ

SAKURA Internet

- BGPの身近なユースケースを紹介しました。
  - 簡単な設定方法を覚えておくと思わぬところで役に立つかもしれません☺
- 弊社インターネットバックボーンにおける流通トラフィックの解析結果より、
- 数年前からの性質の変化、および今後の動向予測について説明しました。
- 不正トラフィック対策へのルーティングテクニックの応用例を示しました。
  - 日々変化する攻撃手法に合わせて、対策も進化させていく必要があります。